

REMARKS

The foregoing Amendment and the following Remarks are submitted in response to the Final Office Action issued on October 28, 2004 and the Advisory Action issued on February 15, 2005 in connection with the above-identified patent application, and are being filed as a Preliminary Amendment along with a Request for Continued Examination.

Claims 106-181 remain pending in the present application, and stand rejected. Independent claims 106, 122, 138, 152, and 168 have been amended to emphasize that the black box is unique and has a public / private key pair and functionality necessary to employ such key pair within the DRM system on the computing device. Applicants respectfully submit that no new matter has been added to the application by the Amendment.

The Examiner has maintained the rejection of claims 106-181 under 35 USC § 103(a) as being obvious over Downs et al. (U.S. Patent No. 6,574,609). Applicants respectfully traverse the § 103(a) rejection insofar as it may be applied to the claims as amended.

Independent claim 106 as amended now recites a method in combination with a digital rights management (DRM) system operating on a computing device, where the DRM system employs a black box for performing decryption and encryption functions. The method is for obtaining the black box by the DRM system from a black box server. In the method, the DRM system requests the black box from the black box server and the black box server generates the black box. As now recited, the generated black box is unique and has a public / private key pair and functionality necessary to employ such key pair within the DRM

system on the computing device. The black box server then delivers the generated black box to the DRM system, and the DRM system installs the delivered black box therein.

Independent claim 122 as amended recites subject matter similar to that in independent claim 106 as amended, but from the point of view of the DRM system. Independent claim 138 as amended recites subject matter similar to that in independent claim 106 as amended, but from the point of view of the black box server. Independent claim 152 as amended recites subject matter similar to that in independent claim 122 as amended, but in the form of a computer-readable medium having computer-executable instructions thereon for performing the method of claim 122 as amended. Independent claim 168 as amended recites subject matter similar to that in independent claim 138 as amended, but likewise in the form of a computer-readable medium having computer-executable instructions thereon for performing the method of claim 138 as amended.

Inasmuch as the Examiner has heretofore considered the recited black box to be merely a set of encryption / decryption keys, Applicants have amended the independent claims of the present application to now recite that the black box includes such keys and the functionality necessary to employ same in a particular manner within the DRM system on the computing device.

In particular, the black box 30 works in conjunction with the license evaluator 36 to decrypt and encrypt certain information as part of the license evaluation function. In addition, once the license evaluator 36 determines that a user does in fact have the right to render the requested digital content 12 in the manner sought, the black box 30 is provided with a decryption key (KD) for such digital content 12, and performs the function of decrypting such digital content 12 based on such decryption key (KD).

Applicants again point out that the Downs reference discloses a system of managing protected content. Each piece of content is in the form of a secure container (SC) which includes the content encrypted by a symmetric key that is in turn encrypted by the recipient's public key, various digests, a digital certificate of the sender, and a signature. As seen in Fig. 1D, a recipient of the secure container employs a device 109 that includes a decryption / re-encryption function 194 that is protected with tamper resistant code technology and that serves the purpose of decrypting and re-encrypting the content in a more amenable format and with a more amenable symmetric key. (Column 79, line 38 – column 80, line 14).

Significantly, although the Downs decryption / re-encryption function 194 acts in many respects as the black box of the present application, such Downs reference does not at all disclose or even recognize that such a decryption / re-encryption function 194 is a black box or the like that includes cryptographic keys and the functionality necessary to employ same in a particular manner within the DRM system on the computing device, as is required by the claims of the present application.

Moreover, the Downs reference does not at all recognize or even appreciate that such decryption / re-encryption function 194 can become compromised over time and thus should be updated on a regular basis with a new a decryption / re-encryption function 194 from an appropriate server. In fact, Applicants again point out that the Downs reference does not even disclose or suggest any method or mechanism by which the function 194 could be so updated, let alone a black box server for updating the decryption / re-encryption function 194.

Thus, and again, Applicants respectfully submit that the Downs reference does not disclose or suggest that the Downs end-user device 109 should or could request an updated system decryption / re-encryption function 194 from an appropriate server, as is required by claims 106 et seq., or that such an appropriate server should or could generate same with a unique public / private key pair and deliver the generated function 194 to the device 109 such that the device 109 installs the delivered function 194 therein, as is also required by claims 106 et seq. Put simply, without appreciating that the function 194 should be updatable, the Downs reference simply fails to disclose or even suggest any mechanism by which such updating can take place.

Applicants note that the Examiner may attempt to infer the delivery and installation of the Downs function 194 as part of the delivery and installation of the Downs system on a user's computing device. However, and significantly, such an interpretation fails inasmuch as such delivery and installation would not be in response to a request for the function 194 from the Downs system, as is required by the claims. Put simply, the Downs system cannot make such a request if such Downs system has not as yet been delivered and installed.

Accordingly, for all of the aforementioned reasons, Applicants respectfully submit that the Downs reference cannot be applied to make obvious independent claims 106, 122, 138, 152, and 168 as amended, or any claims depending therefrom. Accordingly, Applicants respectfully request reconsideration and withdrawal of the § 103(a) rejection.

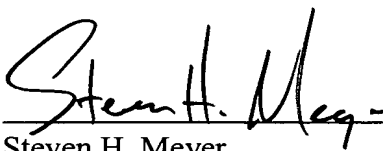
DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

**PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116**

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 106-181, is in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

Date: April 25, 2005


Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439